accenture

Information security checkpoint

Avoid potential security breaches

Protect confidential information & work product

- Any information and materials (tangible or intangible), including Work Product, proprietary or otherwise, which you are privy to as an Accenture employee, falls under Confidential Information*.
- Anything that is made for Accenture and its clients by an employee falls under Work and Work Product*. Both Work and Work Product are owned by Accenture or client and cannot be retained or used by you in a personal capacity. roll off from project.

Read the Terms of Employment and Information Security Policies mentioned below** and consult with supervisor/people advisor as required.

Securely return all Confidential Information and Work & Work Product before leaving Accenture or when you no longer have a business need for it, for example upon

Avoid data theft

- Don't take away or attempt to take away any Confidential Information or Work & Work Product you've received or worked on during your employment with Accenture.
- Don't transfer or store Confidential Information or Work & Work Product to/at locations outside the Accenture and/or client environment.
- Always check with your supervisor before transferring anything out of the client environment even if it is to Accenture.
- Do not transfer any Knowledge Exchange (KX) resources.

Remember Confidential Information and Work & Work Product of Accenture and client cannot be copied or transferred externally without express written authorization for any reason including personal use or reference.

Be transparent and take only what is yours

- Send only required personal files from your Accenture mail ID to personal email ID.
- Double check what you send. Transfer only your personal files such as salary statements, letters etc. and do not share any work-related information.

Don't hide

- Don't use other channels like WhatsApp, Google Drive, personal email, etc. for sending your personal files or any other information.

Watch out for unauthorized access

- Lock your system when unattended.
- Refrain from sharing passwords of system or applications with anyone.
- Ensure that unauthorized users are not permitted access to any confidential or sensitive information of Accenture or clients through you.
- Use only Accenture and client-approved mediums for storage or transfer of information if at all required to do so.

Prevent unauthorized disclosure

- Report any phishing mails received.
- Whenever sending any information, check if the recipient is authorized to receive it.
- Refrain from uploading any confidential information or Work Product on 3rd party websites like WhatsApp, GitHub, Google Drive, etc.
- If requested for confidential information, always validate the user's identity and seek permission from supervisor before sharing.

*For ease of understanding, a conceptual idea of Confidential Information and Work & Work Product is presented in this document. You must continue to adhere to your obligations on Confidentiality and Intellectual Property as mentioned in the terms of employment. The above list is only indicative.

** You are reminded to comply with requirements of all Information Security Policies including Confidentiality, Intellectual Property, Data Privacy, Data Management and Acceptable Use of Information, Devices and Technology Policies and associated policies referenced in any of the above. Visit Protecting Accenture for resources on how to stay compliant with Information Security.

You are obligated to protect Accenture's and client's Confidential Information even after your last working day at Accenture.

Information security breaches are costly and can damage Accenture's brand and relationship with clients. It can also be violative of organizational policies and result in appropriate actions. Exercise good judgement when handling information and reach out to supervisors and people advisor when in doubt.